مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Large-Scale Brute-Force Attacks Targeting VPN Services

Tracking #:432315774

Date:19-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security council has observed that Cisco warns of a rise in brute-force attacks hitting VPN and SSH services worldwide.

TECHNICAL DETAILS:

Cisco Talos is warning organizations of a large-scale brute-force attack campaign targeting VPN and SSH services on various devices including Cisco, CheckPoint, Fortinet, SonicWall, and Ubiquiti. Attackers are attempting to gain unauthorized access by trying numerous username and password combinations.

Brute-force attacks involve systematically trying different username and password combinations until gaining access to an account. If successful, attackers can hijack devices or access internal networks. Successful brute-force attacks can lead to:

- **Unauthorized Network Access:** Hackers can use compromised credentials to gain access to your internal network and steal sensitive data.
- **Account Lockouts:** Repeated login attempts can trigger account lockouts, hindering legitimate users.
- **Denial-of-Service (DoS):** A surge in login attempts can overwhelm VPN servers, making them unavailable for authorized users.

Campaign Details:

- **Targets:** VPN and SSH services on Cisco, CheckPoint, Fortinet, SonicWall, and Ubiquiti devices.
- **Start Date:** Since at least March 18, 2024
- **Attack Methods:**
  - Brute-forcing login attempts with a mix of valid and generic usernames.
  - Originates from anonymizing services like TOR and proxies to evade detection.
- **Potential Impacts:**
  - Unauthorized network access.
  - Account lockouts (preventing legitimate users from accessing accounts).
  - Denial-of-service (DoS) attacks (overwhelming systems with login attempts).

Affected Services:

The following VPN and SSH services are being targeted:

- Cisco Secure Firewall VPN
- Check Point VPN
- Fortinet VPN
- SonicWall VPN
- RD Web Services
- MikroTik
- Draytek
- Ubiquiti

Cisco also warned of password spray attacks targeting remote access VPN services. According to researchers, it is a part of reconnaissance efforts.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- **Implement strong password policies:** Enforce complex passwords with minimum length requirements and regular password changes.
- **Enable multi-factor authentication (MFA):** MFA adds an extra layer of security by requiring a second verification factor beyond a username and password.
- **Patch and update systems:** Ensure all systems and software are up-to-date with the latest security patches.
- **Monitor login attempts:** Monitor your system for unusual login activity and investigate suspicious attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/